



	Hojas ->	Ej.1	Ej.2	Ej.3	Ej.4	
		1	1	1	1	
	Calif. ->	B	2	B	B	Final (A)

Todas las respuestas se consideran válidas solo si están debidamente justificadas.

Ejercicio 1

Una conexión TCP pasa por un router intermedio que captura los siguientes paquetes:

Source	Destination	Info
192.168.100.40	192.168.100.35	3324 > 4443 [FIN,ACK] Seq=892 Ack=1954 Len=0
192.168.100.35	192.168.100.40	4443 > 3324 [FIN,ACK] Seq=1954 Ack=893 Len=0
192.168.100.40	192.168.100.35	4443 > 3324 [ACK] Seq=893 Ack=1955 Len=0

- Suponiendo que el host 192.168.100.35 envió un total 954 bytes y el host 192.168.100.40 un total de 92 bytes, muestre una posible secuencia de intercambio de segmentos desde que comienza la conexión hasta que llega al primer segmento de la trama capturada por el router.
- Ahora suponga que el router intermedio desecha el último segmento capturado, explique los eventos que suceden en ambos extremos de la conexión a partir de éste descarte, detallando los cambios de estados hasta que llegan al estado CLOSED.

Ejercicio 2

Una conexión recién establecida tiene un RTT=100ms y debe transmitir 70KB. El receptor siempre anuncia una *Advertised Window* de 64KB y se sabe que el proveedor de servicio del host emisor limita la velocidad descartando todos los segmentos de una ráfaga si se envían 32KB o más por RTT.

- ¿Cuántos datos lleva transmitidos con éxito (i.e.: datos que ya no están "en vuelo") y cuántos están en vuelo a los 450ms?
- Si a partir de los 650ms de iniciada la transferencia, la red desordena todas las ráfagas de segmentos que envía el emisor, de manera que el primer segmento siempre llega al final manteniendo el orden del resto de los segmentos de la ráfaga, ¿En qué instante se activa el algoritmo de *Fast Recovery* / *Fast Retransmit*?

Ejercicio 3

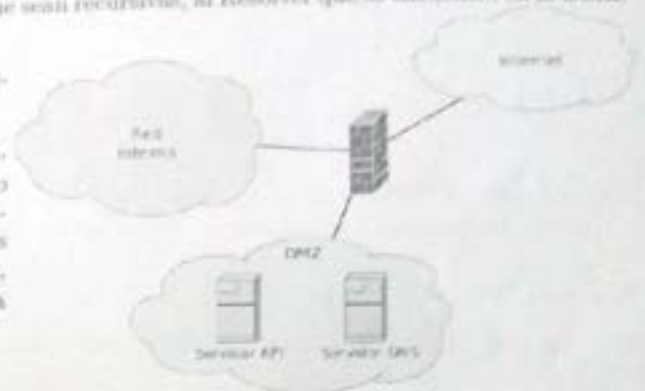
Desde los laboratorios de una universidad, los hosts acceden a los sitios Web usando un proxy Web (que comienza con la cache vacía). En un instante dado desde un host se accede a <http://www.onlyonepicture.com/index.html>. Inmediatamente después de recibidos todos los recursos HTTP, se accede desde otro host en otro laboratorio al mismo recurso en el mismo sitio Web. Sabiendo que todos los navegadores y servidores usan HTTP/1.1, y que *index.html* es una página Web cuyo código HTML tiene 800 bytes y sólo contiene dos imágenes de 1200 bytes cada una:

- Indique la cantidad de RTTs TCP generados por el acceso desde el primer host, teniendo en cuenta que los segmentos TCP pueden enviar hasta 2KB de datos. Suponer que los RTTs entre todos los hosts son iguales.
- Suponiendo que los recursos HTTP no son modificados, muestre todos los mensajes HTTP que desencadena el acceso desde el 2do host.

Ejercicio 4

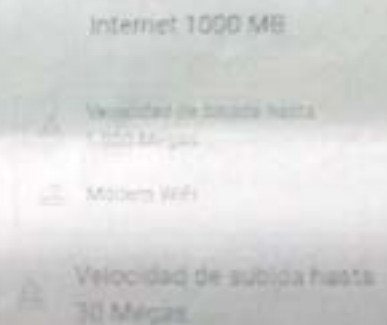
En la figura se muestra la organización de red de una compañía. En la DMZ se encuentran un servidor DNS, que funciona como Resolver para la Red Interna de la compañía, y un servidor exponiendo una API en el puerto 29956. El servidor API es el único al que se puede tener acceso desde Internet. Los empleados desde la red interna pueden visitar sitios web usando HTTP o HTTPS, pero sólo pueden realizar consultas DNS que sean recursivas, al Resolver que se encuentra en la DMZ.

- Definir las reglas del firewall para que se cumplan los requerimientos mencionados.
- Para poder realizar consultas DNS de manera segura se desea implementar un sistema que permita garantizar la integridad y no repudio de las respuestas que el Servidor DNS le envía a los dispositivos en la Red Interna. Explicar cómo se firman los mensajes en el servidor y que debe hacer el cliente para validar la firma, aclarando qué información debe tener previamente instalada cada dispositivo.



Ejercicio 5 (Opcional)

Tienes un vecino (edificio) y amigo que estudia física, ambos contrataron el mismo servicio de internet (banda ancha) a la misma empresa (acceso via línea de par de cobre de la telefonía fija). En su pagina web figuran estos datos del servicio: (ver figura a la derecha, fue traducida por Google translate). Por tu lado averiguaste (ya que tienes contratado el mismo servicio) que el cablemódem ADSL (G. Fast) tiene "incluido" un "router" Wi-Fi 5 (IEEE 802.11ac Wave 1) cuyo "Max Data Rate" recordas de tus clases de redes que llega a 1.3 Gbps (en 80 Mhz y modulando a 245 QAM) PHY Rate (ver figura más abajo). La cuestión que se encuentran en el hall del edificio y enseguida comienza a quejarse del servicio 1000 MB (en realidad es 1000 Mbps) y que hace los números y no le cierran los cálculos que tarda en bajar unos archivos de varios TBytes de datos vía FTP desde un servidor en la UBA Edificio Infinito + Cero, vos le aclaras que tiene una explicación ese comportamiento en la performance. Acto seguido te pide que le expliques (recordar que estudia física) porque tiene esa performance.



¿Podrías detallar a continuación que explicación le darías a tu amigo por que no tiene la performance esperada por él en la bajada de sus archivos de datos? Y si además existe alguna limitación de cómo el proveedor del servicio brinda el mismo.

	802.11n	802.11n	802.11ac Wave 1
	IEEE Specification		Today
Band	2.4 GHz & 5 GHz	2.4 GHz & 5 GHz	5 GHz
MIMO	Single User (SU)	Single User (SU)	Single User (SU)
PHY Rate	450 Mbps	600 Mbps	1.3 Gbps
Channel Width	20 or 40 MHz	20 or 40 MHz	20, 40, 80 MHz
Modulation	64 QAM	64 QAM	256 QAM
Spatial Streams	3	4	3
MAC Throughput*	293 Mbps	290 Mbps	243 Mbps

* Assuming a 80% MAC efficiency with highest MCS

Ej) a) After Practice. Ahora a la hora de lo siguiente:

B~~A~~ = 192.168.100.40:3324

A~~B~~ = 192.168.100.35:4443

(B)

2	b
8	B

⇒ Suponemos que el HOST A envió un total de 954 Bytes y B~~A~~ envió un total de 92 Bytes, mientras una posible secuencia de intercambio de segmentos debido que comienza la conexión entre que llega el primer segmento de B a A. Transmite el paquete X al Host. Voy a suponer que el Host A envía el paquete X.

ORG	OST	FLAGS	#SEQ	ACK	LENGTH
A	B	SYN	999		0
B	A	SYN+ACK	299	1000	0
A	B	ACK	1000	900	0
A	B	ACK	1000	900	954 B
B	A	ACK	999	1954 ✓	0
B	A	ACK	999	1954	92 B
A	B	ACK	1954	892 ✓	0
B	A	FIN+ACK	892	1954	0

⑥ El número de segmentos transmitidos (Trans).
 $799 + 92 + 1 = 892$
 $800 + 92 + 1 = 893$

⑦ Terminó el 3-WAY HANDSHAKE.

b) Ahora hipotetizando que el Router intermedio devuelve el último segmento grabado, explique los eventos que suceden en ambos extremos de la conexión a partir de este momento, detallando los cambios de estado host que llegan a CLOSED.

→ Al menos 1, 2) y 3) a los tramos grabados → Antes de 4 Ambos SOCKETS están en ESTABLISHED.

En 1) El Host B toma la iniciativa y decide cerrar la conexión x B que pasa de ESTABLISHED a FIN_WAIT_1.

En 2) A recibe el cierre de la conexión de B y envía un FIN+ACK, pasando de ESTABLISHED a CLOSE_WAIT y luego a LAST_ACK.

En 3) B recibe el FIN+ACK de A x B que el pasa de FIN_WAIT_1 a TIME_WAIT.

Perd, el PERDERSE 3) A después en LAST_ACK → EXISTEN 2 escenarios posibles.

1- A Recibe el Timeout porque xq no regresaron la Fin, entonces B reenvía y si B no recibe la conexión puede volver a enviar 3. (luego A recibe y responde a CLOSED Δ) y B también luego de un "retrans" Δ).

2- A Recibe el Timeout porque xq no regresaron la Fin, entonces B reenvía y en este caso B recibe la conexión, x B que A recibe un RST y se cierra abruptamente la conexión.

Δ ~~después de~~ 2 segmentos lifetime
 Δ luego de 2 segmentos lifetime.

Problema

74
16/11/22

gd) una buena Red de redes tiene un RTT = 100 ms y debe Transmisor 70KB. El Receptor siempre envía una RWND = 64KB y se sabe que el proveedor de servicios del Host emisor limita el ancho de banda de la red. Todos los segmentos de una Pajera se le envía 32KB más x RTT.

a) ¿Cuántos Datos lleva Transmisor en élite y cuánto está en vuelo a los 450 ms?

⇒ IW = 2 · MSS = 4KB 1 MSS = 2KB RWND = 64KB
SSTHRESH = 64KB, O el resto x Pajera de 32KB o más.
RTT = 100 ms, a Transmisor 70KB.

RTT	CWND	SSTHRESH	RWND	FLIGHT SIZE	LBS	LBACK
1	4KB	64KB	64KB	4KB	4KB	0
2	8KB	64KB	64KB	8KB	12KB	4KB
3	16KB	64KB	64KB	16KB	28KB	12KB
4	32KB	64KB	64KB	32KB	60KB	28KB
450ms → 5	32KB	64KB	64KB	32KB	60KB	28KB

RTT Según el variables informados tengo 28KB y en vuelo 32KB.

Alto que como tiene 2 Falsos (RTT) un Receptor ACK nuevo en el 6RTT, también un Receptor de 6 bytes

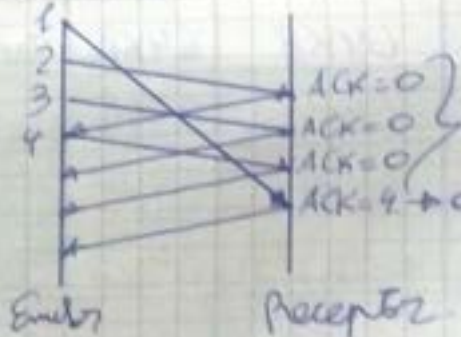
b) Si a partir de 650ms de inicio de transferencia, el Recd. detecta todos los segmentos de segmentos que avanza el emisor, de manera que el primer segmento llega al final manteniendo el orden del Recd de los segmentos de la pila en que continúa lo activo el algoritmo de Fast Recovery / Fast Retransmit?

RTT	CWND	SSTHRESH	RWND	Flight Size	LBS	IBACK
6	4KB	16KB	64KB	4KB	32KB	28KB
7	8KB	16KB	64KB	8KB	40KB	32KB
8	4KB	4KB	64KB	4KB	44KB	36KB
9			64KB			
10			64KB			

→ 2KB

→ 4KB

Se activa en el RTT 7 (1 primer seg, 6 bytes por byte si tenía que especificar en los RTT o lo hab en el 7), seg en el 7 RTT envía 4 Segmentos / transmit



Se activa el FR/R
→ de la x el retransm de los datos.

→ Al recibir los nuevos datos
CWND = SSTHRESH.

Según el protocolo $SSTHRESH = \frac{Flight Size + 2 * MSS}{2}$
→ $MAX(4KB, 4KB) = 4KB$

(B)

3/4

16(11/22)

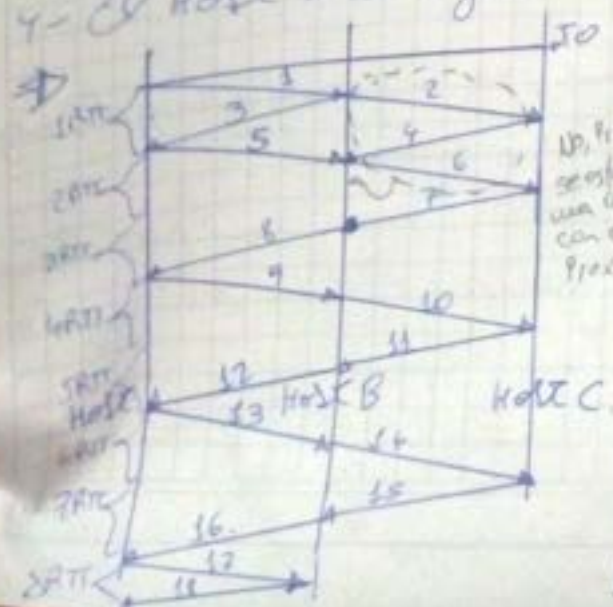
Ep) Desde la librería de la universidad, los hosts acceden a la página WEB de un Proxy WEB. En un instante un Host accede a `HTTP://WWW.ONLYPICTURES.COM/INDEX.HTML`.

Inmediatamente después de recibir el recurso HTTP, se accede desde otro host a otra biblioteca de nuevo recurso en el mismo sitio web. Sabiendo que todo el navegador y la web browser usan HTTP/1.1 y que el Index.HTML es un página web cuyo código HTML tiene 800 Bytes y los otros 2 imágenes de 1200 Bytes cada una.

a) Indique el total de RTT's TCP generados al acceder desde el Primer Host, teniendo en cuenta que los segmentos TCP pueden tener hasta 2KB de datos. Suponga que los RTT's entre todos los Hosts son iguales.

Se genera ~~una~~ máquina involucrada.

- 1- El Host A (El primer host que accede a primera vez).
- 2- El Host B (El Proxy)
- 3- El Host C que tiene la página o todo el Resource.
- 4- El Host D (El segundo host en el otro biblioteca).



- 1- Envío el SYN al Proxy
- 2- El Proxy envía el ACK al servidor
- 3- El Proxy responde con ACK+SYN
- 4- El servidor responde con ACK+SYN
- 5- El Host A envía el pedido de página
- 6- El proxy pide la página al servidor
- 7- El servidor le da de al proxy
- 8- El proxy le da de al Host A
- 9- El Host A le pide la primera imagen
- 10- El proxy le pide al servidor
- 11- El servidor le da de al proxy
- 12- El proxy le da de al Host A

- 13- El Host A pide el recurso index al proxy
- 14- El proxy le pide al servidor
- 15- El servidor le da el proxy
- 16- El proxy se lo da al HOST A

17- Envío de 12 bytes de HTML.

(Juego de protocolo en el navegador, entre los BTT's con el tiempo de ida que pide enter, por acceder al sitio web que el (servidor en Google) @, obteniendo los BTT con un valor de tiempo (Es decir RTT = RTT), luego a que devuelva, 8 BTT en ~~completo~~ transferencia y volver a Google.

b) Suponiendo que los Recursos HTTP no son modificables, muestra cómo los mensajes HTTP que se envían al 200 HOST. El HOST O genera y recibe el siguiente mensaje.

GET: /INDEX.HTML HTTP/1.1

HOST: WWW.ONLYONEPICTURE.COM/

El proxy recibe esto y lo envía al servidor (HOST O)

GET: /INDEX.HTML HTTP/1.1

HOST: WWW.ONLYONEPICTURE

LAST-MODIFIED: (El Fecha y hora de la última actualización)

Response: 200 OK

~~El proxy~~ le envía que no fue modificado

Response: 200 OK

DATA: /INDEX.HTML

Lo mismo sucede con los 2 mensajes, ya que no se modifican y el proxy

le da al HOST O los 2 mensajes que tenía almacenados

4 GET y 4 Response (2 del HOST O al proxy y 2 del proxy al servidor, 2 Response al proxy desde el servidor y 2 Response del proxy al HOST O)

pero no puede decir, no me da el tiempo.

Recordando en JS ya le da mi Google, diciendo que no se puede mi AHT.

(B)

4/4

16/11/22

g4) a) Definir las reglas de Firewall por las que se cumplen las req. mencionadas.

Stratificación

Al ser en FW de 3 pases, la Prefectura de la siguiente forma.

- 1- Los puertos IP de la RED INTERNA/LAN de 192.168.1.0/24
- 2- Si uno * de un puerto superior a 1024.
- 3- Luego de validar la dirección el servidor IP, se expone a Internet.

Redes \ A	LAN (R1)	DMZ	Internet
LAN (R1)	X	UDP (pusher) /	HTTP y HTTPS /
DMZ	Drop.	X	Pusher (UDP) /
Internet	Drop.	API (G) /	X

Política x Defecto
Drop. /

Reglas de FW.

$\langle 192.168.1.0/24, *, DMZ(Pusher), 53, UDP \rangle$ /

$\langle 192.168.1.0/24, *, Internet, 80, TCP \rangle$ No se permite HTTP /

$\langle 192.168.1.0/24, *, Internet, 443, TCP \rangle$ No se permite HTTPS /

$\langle DMZ, *, Internet, 93, UDP \rangle$ Validar DNS a Internet /

~~Drop~~

$\langle Internet, *, DMZ(Servidor API), 29.956, TCP \rangle$ /

b) Para poder realizar consultas DNS de manera segura se debe implementar un sistema que permita garantizar la integridad y no REPUDIO de las respuestas que el servidor DNS le envía a la Resp de la RI. Explicar cómo se firma el mensaje en el servidor y qué debe hacer el cliente para validar la firma, aclarando qué info debe tener previamente instalado en el cliente.

Las preguntas son del servidor DNS a la Resp de la RI.

Para ello se necesita lo siguiente:

- 1- Que la Resp de la RI y el servidor DNS, compartan una función de HASH (ej SHA-512).
- 2- El servidor debe tener su clave privada y pública.
- 3- Que con Disponibles de la RI tenga instalada la clave pública del servidor.

Forma de Responder:

- 1- El cliente envía su petición junto con su usuario, al servidor.
- 2- El servidor hace la consulta, a eso le hace un Digest con la HASH Función de HASH (el resultado y el usuario).

3- A ese Digest lo ~~hace~~ ~~encrypt~~ ~~en~~ la clave privada y lo envía al usuario que lo hizo la consulta (junto con la consulta sin encrypt).

4- El usuario desencripta el mensaje recibido con la K_S^+ (del servidor) y obtiene el HASH de la consulta + su usuario.

5- Hace un HASH de su usuario, lo ~~respuesta~~ (a la consulta DNS) y lo ~~compara~~ con la ~~distancia~~ en la respuesta del servidor (el Digest que hizo el servidor con la consulta y su usuario).

6- Si coinciden perfecto.

El servidor encrypta el HASH con la K_S , garantiza que al hacerlo desencriptar con la K_S^+ , esto garantiza NO REPUDIO y el que coincide el HASH enviado con el generado x el usuario, garantiza integridad.